IBM **Guardium**
Discover and Classify

POLICY ENGINE USER GUIDE

IBM GUARDIUM DISCOVER AND CLASSIFY

VERSION 4.2.2

TABLE OF CONTENTS

POLICY ENGINE OVERVIEW

The IGDC platform allows you to add and manage use cases/policies for IGDC integrations with other tools and services. The integrations are handled in the **Policy Engine** and **Ecosystem > Marketplace** tools.

Table 1: Supported Integrations

INTEGRATION PRODUCT	USE CASE
Alation	Enrichment of the Alation data catalog (Data source export) The integration app exports data sources from IGDC data source catalog to the Alation data catalog as assets. This ensures the Alation's data governance capabilities cover all your data assets.
	Enrichment of the Alation data catalog with topology (Data source export) The integration app exports the data source schemas, tables and columns from IGDC to the Alation assets.
	Enrichment of the IGDC data source catalog (Data source import) The integration app imports the assets from the Alation data catalog to the IGDC data source catalog for further classification and cataloging. This facilitates identification and classification of sensitive data by IGDC
Collibra Data Intelligence Cloud	Enrichment of the Collibra assets The integration app creates a new asset in Collibra when IGDC discovers a file/table with sensitive data. This helps you to ensure the sensitive data is monitored and is in compliance with appropriate policies and regulations.
IBM Guardium Data Protection	Import GDP data sources into IGDC for further scanning.
	Automate Groups and Policies creation based on IGDC discovery results.
	Aggregate data source discovery and vulnerabilities scan and send them to IGDC for reporting capabilities. IGDCvisualizes the overall security status of your organization's data sources in graphical form and has the ability to dive in to the data sources list for the further investigation and generate reports in CSV and XLS formats to be imported to other protection tools that your organization uses.
MS Purview	Import sensitivity labels to IGDC The integration app automatically imports sensitivity labels from MS Purview to IGDC. These labels will appear as sensitivity classes in IGDC , and can be mapped to data elements and document classifiers. IGDC populates the automatically imported sensitivity labels for the criticality score configuration.
OneTrust	DSAR request creation & population The integration app creates a DSAR request in OneTrust and uses IGDC to populate it with enriched data.
ServiceNow	Report IGDC discovery results to ServiceNow as incidents The integration app automatically creates an incident in ServiceNow if the number of sensitive data locations in a data source is over a preconfigured number (threshold) or if sensitive data like personal or credit card information is present.
Portal26 (Titaniam) Spectra	Automatic encryption of files containing personal data hosted in Amazon S3 bucket After IGDC analyzes the S3 bucket and discovers personal data in files stored there, the integration app will automatically encrypt these files.
	File tagging/labeling for encrypted objects in S3 buckets To provide context for the encrypted files in the S3 bucket, the integration app can assign tags (labels) to the files with useful information. For example, data elements and categories discovered by IGDC in the file.
	Reports on workflow behavior, metrics of encrypted files, amount of pass/fail and reasons for failed results The integration app can keep track of progress of the workflow (how many files Portal26

INTEGRATION PRODUCT	USE CASE
	tried to encrypt and how successful it was), as well as log the affected resources.
Splunk	Monitor Sensitive Data The integration app sends an alert to Splunk if a configured data element(s) was discovered by the product plugin.
	Monitor Sensitive Data in Motion The integration app sends an alert to Splunk if a configured data element(s) was discovered in data-in-motion.
	Monitor New Sources of Sensitive Data The integration app sends an alert to Splunk if a new data source is discovered by the Network Analytic Engine, which classifies data-in-motion.

INTEGRATION INSTALLATION AND CONFIGURATION

The prerequisite to building policies in IGDC is having all the necessary integrations installed and configured.

For instructions on how to install, upgrade, and remove an integration, see the relevant integration's guide.

To configure connection to the integrated instance, go to the **Marketplace**. This page provides the overview of the available integrations, gives their current status, and assists in configuring the connection to the integrated instance.

BUILDING POLICIES

The **Policy Engine**focuses on creating and editing the desired policies based on your configured integrations. You can include several integrations/use cases in a single policy to cover the desired regulation/type of data you wish to handle. You can set one or several conditions that will activate when the policy is triggered.

- Data elements: IGDC discovers the specified data element(s) in a data source, e.g. credit card number, passport number, etc.
- Data category: IGDC includes a data source in the specified data category(ies), e.g. financial information, contact information, etc.
- Regulation: IGDC tags a data source by the specified regulation(s), e.g. PCI DSS, GDPR, etc.
- Data source type: IGDC discovers a specified data source type, e.g. database, cloud storage, etc.
- Data source URL: IGDC discovers a data source with the specified URL.

For example:

You have configured 3 IGDC integrations: Alation, Portal26, Splunk.

In the Policy Engine, you can create a single policy for PCI DSS regulation, which involves the 3 integrations. Once IGDC "tags" a file in Amazon S3 bucket as belonging to PCI DSS regulation, the event will trigger the following actions:

1. IGDC will create an asset in Alation for the S3 bucket and will export the topology info as metadata to the created Alation asset.

2. Portal26 will encrypt the tagged file in the Amazon S3 bucket.

3. IGDC will send an alert to Splunk about the event.

INTEGRATIONS CONFIGURATION IN ECOSYSTEM

In **Ecosystem > Marketplace**, you can review the integration options for the IGDC solution. The page shows a list of tools available for integration with IGDC. It also gives the ability to search for apps by name (**1**) and filter (**2**) them by category, vendor and status.

Table 1: Marketplace integration properties

PROPERTY	DESCRIPTION
Name (Search)	Name of the integration app in the Marketplace. For example: Collibra Data Intelligence Platform You can search by name using the search bar (**1**).
Category (Filter)	Integration category. IGDC groups the integration apps by function into categories. For example, ticket creation, event management, etc. You can filter the displayed apps by category using the sidebar filters.
Product (Filter)	Vendor of the integrated tool, e.g. Splunk, Collibra, etc. You can filter the displayed apps by product using the sidebar filters.
Status (Filter)	Current status of the integration app. The status is represented by the icon in the upper right corner of each integration's pane. Options: Not configured, Live, Failed. **Not configured** (): The integration app is not installed or settings are missing in the Configuration tab. **Live** (): The integration is installed and configured, IGDC successfully connected to the integration app destination. **Failed** (): The integration app failed to connect to the destination instance. You can filter the displayed apps by status using the sidebar filters.

Figure 2: Ecosystem page

Click the desired product to learn more about its integration with IGDC. On the integration page, you will see the integration status (**1**), brief description and the business value of the integration in the **Overview** tab (**2**), and configuration fields in the **Configuration** tab (**3**).

Figure 3: Integration product page in the ecosystem

COLLIBRA CONFIGURATION

The Collibra Data Intelligence Cloud works closely with various Infrastructure-as-a-Service cloud providers to create a flexible and secure environment for metadata management and data governance.

IGDC discovers data sources, analyzes them, and classifies sensitive data in the data sources.

This integration app is an extension of IGDC capabilities. It offers an automated way to enrich Collibra assets with sensitive data and metadata from this platform.

To configure the app settings, go to **Ecosystem > Collibra Data Intelligence Platform**. Then select the **Configuration** tab and configure the app settings.

Table 1: Collibra configuration

PARAMETER	DESCRIPTION
Collibra's Base URL	Hostname of the Collibra instance. *(Required)*
Username for Collibra instance	Username of the designated user with admin access to Collibra. *(Required)*
Password for Collibra instance	Password of the designated user with admin access to Collibra. *(Required)*

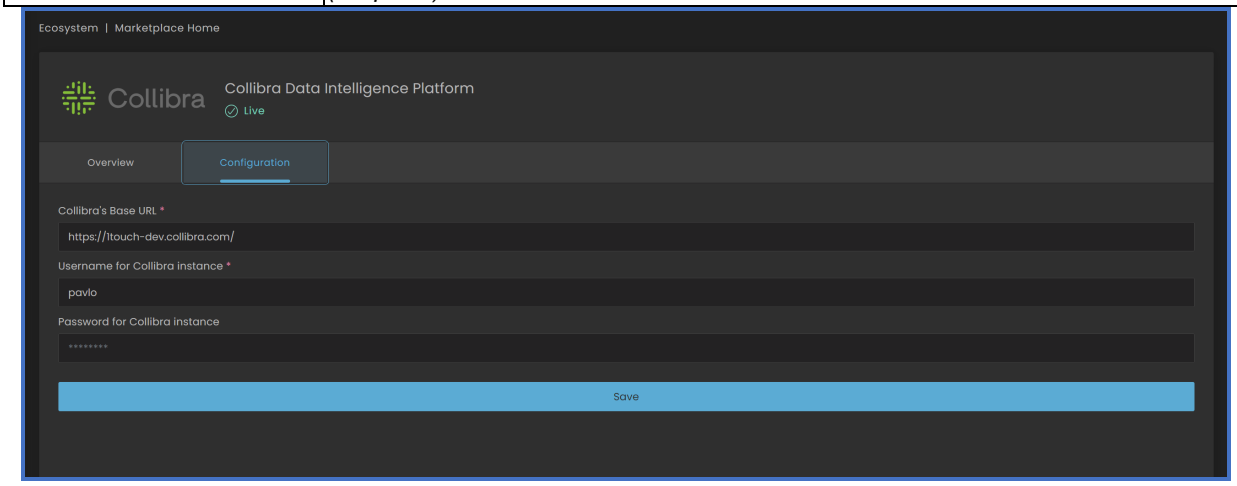


Figure 2: Collibra configuration

GOOGLE LABELING CONFIGURATION

This integration enables the automatic labeling of files in Google Drive based on the personal data they contain, allowing users to manage their data more efficiently and ensure compliance with privacy regulations.

To configure the app settings, go to **Ecosystem > Google labelling for DLP enhancement**. Then select the **Configuration** tab and configure the app settings.

Table 1: Google labeling configuration

PARAMETER	DESCRIPTION
Google account secret	Email of the designated google account. *(Required)*
Google account client secret file	Content of the secret file from the designated Google account.

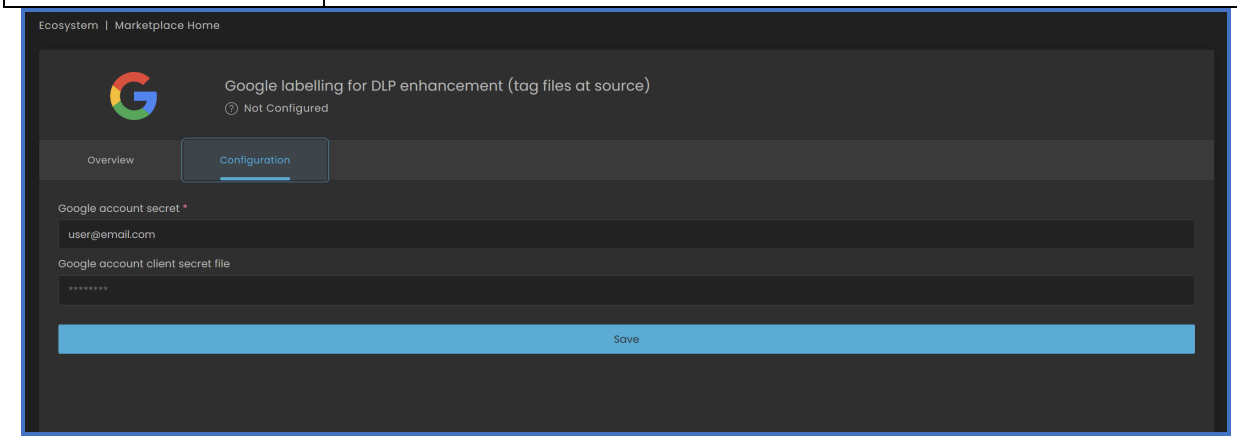


Figure 2: Google labeling configuration

IBM GUARDIUM DATA PROTECTION (GDP) POLICY ENGINE CONFIGURATION

The mutual product of IGDC and IBM, Guardium Data Protection (GDP) combines the best data discovery and protection mechanisms to provide valuable security insights based on the information collected by both platforms.

IGDC classifies sensitive data from across the enterprise. GDP provides real-time data activity monitoring and advanced user behavior analytics to help discover unusual activity around sensitive data.

This integration enables the pulling and pushing of data from and into Guardium Data Protection and IGDC to provide context around data source inventory in IGDC.

To configure the app settings, go to **Ecosystem > IBM Guardium Data Protection**. Then select the **Configuration** tab and configure the app settings.

Table 1: GDP configuration

PARAMETER	DESCRIPTION
Guardium host	Hostname of the GDP instance. *(Required)*
Guardium Port	GDP instance port number. *(Optional)*
Guardium Scheme	Web scheme used by the target GDP instance. Options: https, http. *(Optional)*
Guardium client_id	Oauth client id of the GDP instance. *(Required)*
Guardium client_secret	Oauth client secret of the GDP instance. *(Required)*
Guardium username	Username of the designated user with access to GDP. *(Required)*
Guardium password	Password of the designated user with access to GDP. *(Required)*
Guardium cli_password	GDP CLI user password required for Oauth setup. *(Required)*
Guardium database_vendor group name	Name of the GDP group to store the scanned vendors. *(Required)*
Guardium host group name	Name of the GDP group to store the scanned hostnames. *(Required)*
Guardium database group name	Name of the GDP group to store the scanned database names. *(Required)*
Guardium tablename group name	Name of the GDP group to store the scanned table names. *(Required)*
Guardium general group name	Name of the GDP group to store the scanned databases, hostnames, ports. *(Required)*
Guardium install policy	Property that defines whether GDP will automatically trigger the mapping policies. Options: yes; no. *(Required)*

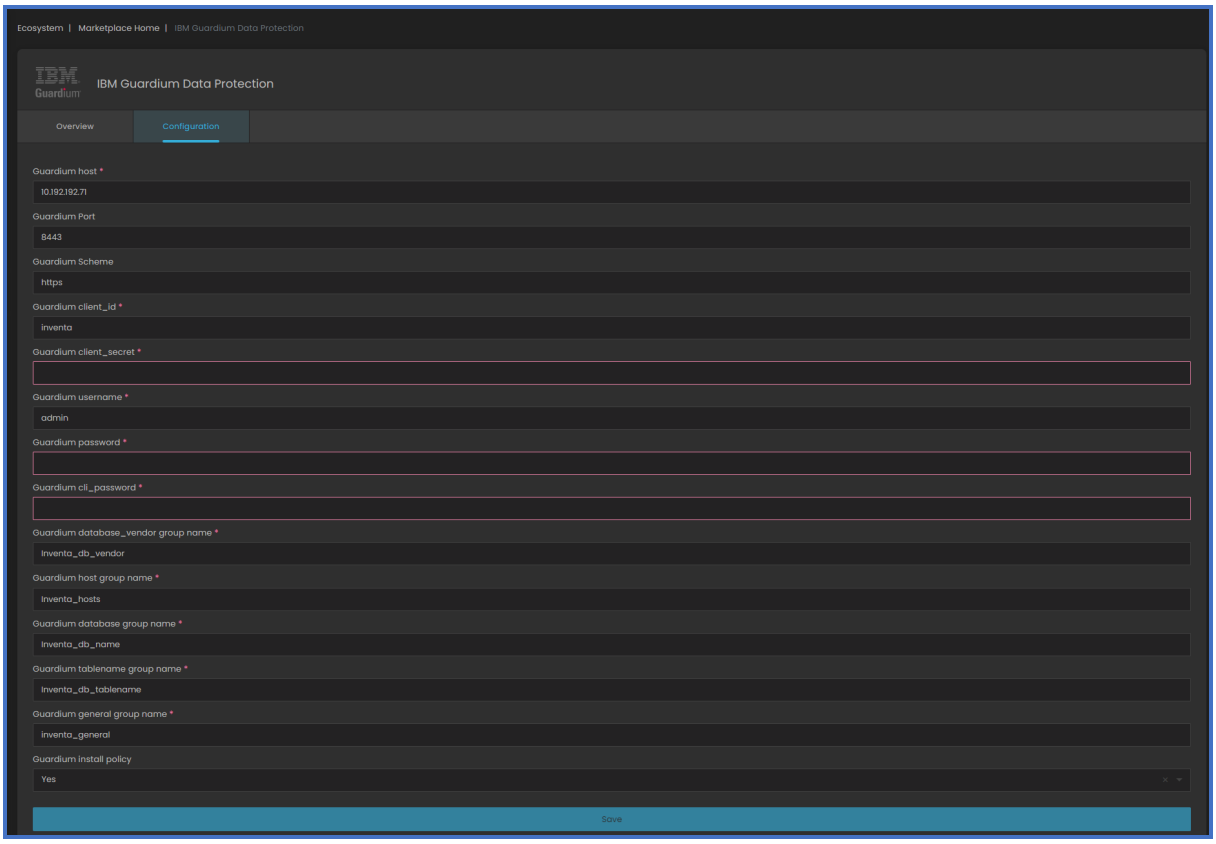


Figure 2: IBM GDP configuration

MICROSOFT AZURE INFORMATION PROTECTION (AIP) CONFIGURATION (MS PURVIEW)

This page allows for the configuration of IGDC's integration with Microsoft Azure Information Protection (AIP), which is a part of Microsoft Purview.

Microsoft Purview is a family of data governance, risk, and compliance solutions that can help your organization govern, protect, and manage your entire data estate. Microsoft Purview solutions provide integrated coverage and help address the recent increases in remote user connectivity, the fragmentation of data across organizations, and the blurring of traditional IT management roles.

This integration's purpose is to utilize MS AIP sensitivity labels functionality and communicate with IGDC in order to scan Microsoft resources like Azure DBs, OneDrive, and Exchange and assign corresponding labels to the data elements within and outside the MS resources.

To configure the app settings, go to **Ecosystem > Microsoft Azure Information Protection**. Then select the **Configuration** tab and configure the app settings. All fields are required.

Table 1: Microsoft Azure Information Protection (MIP) configuration

PARAMETER	DESCRIPTION
Microsoft client id	Client ID of the designated user with access to MS Purview and MS AIP. It can be obtained from the registered app details. For, details refer to Quickstart: Register an application with the Microsoft identity platform.
Microsoft client secret	Client secret of the designated user with access to MS Purview and MS AIP. For, details refer to Quickstart: Register an application with the Microsoft identity platform.
Microsoft tenant id	Tenant ID of the designated user with access to MS Purview and MS AIP. It is configured when registering the app. For, details refer to Quickstart: Register an application with the Microsoft identity platform.
Enabling importing labels	Enable/disable import of sensitivity labels from MS AIP to IGDC.
Activate labelling task	Enable/disable assigning sensitivity labels in MS AIP.

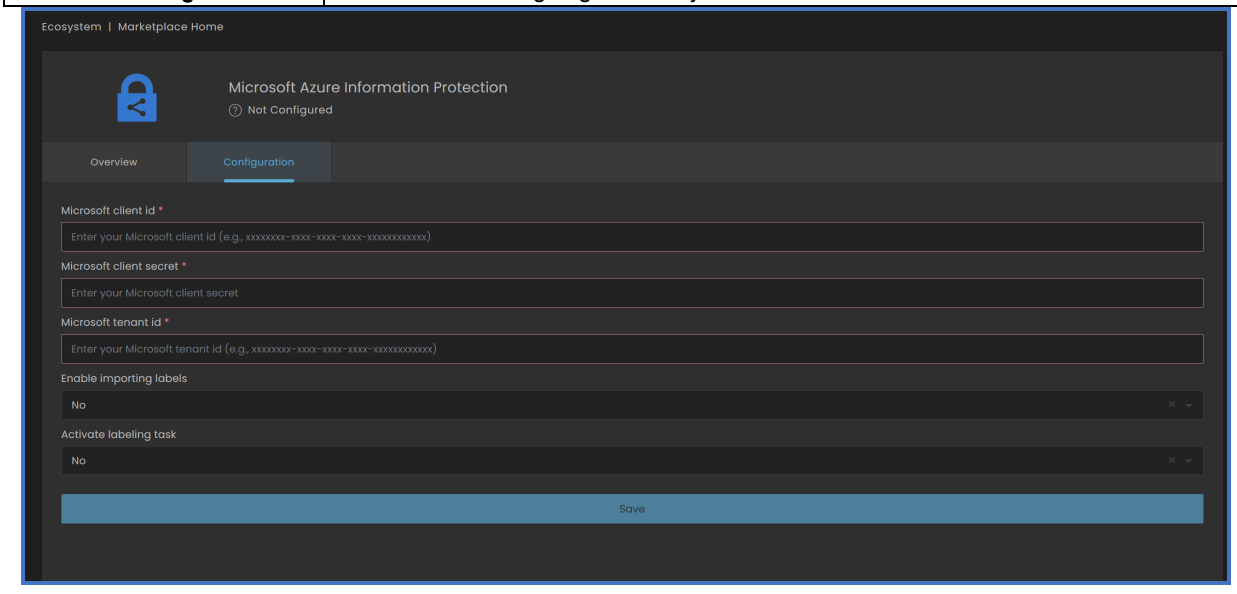


Figure 2: MS AIP configuration

ONETRUST CONFIGURATION

OneTrust is a solution used to help organizations implement compliance and risk management initiatives. It works across many key stakeholders to transform compliance, reduce risk, increase business value, and competitively differentiate your business. Through a central data model, agile workflows, and value-based reporting, OneTrust helps manage: privacy, security, risk, ethics and compliance, legal, data and analytics, marketing, finance, and sustainability.

This integration's purpose is to utilize OneTrust's DSAR requests and communicate with this discovery & classification solution in order to provide relevant discovered data subject info to the OneTrust system.

To configure the app settings, go to **Ecosystem > OneTrust**. Then select the **Configuration** tab and configure the app settings.

Table 1: OneTrust configuration

PARAMETER	DESCRIPTION
OneTrust's Base URL	Hostname of the OneTrust instance. *(Required)*
Client ID for OneTrust instance	Client ID of the designated user with access to OneTrust. *(Required)*
Client secret for OneTrust instance	Client secret of the designated user with access to OneTrust. *(Required)*
Working status of a subtask to be processed	Status of the OneTrust subtask, which initiates OneTrust interaction with IGDC via the integration app. *(Required)*
Timeout between attempts to collect and process requests in OneTrust	Timeout in seconds between scanning the OneTrust instance for relevant requests. *(Optional)*

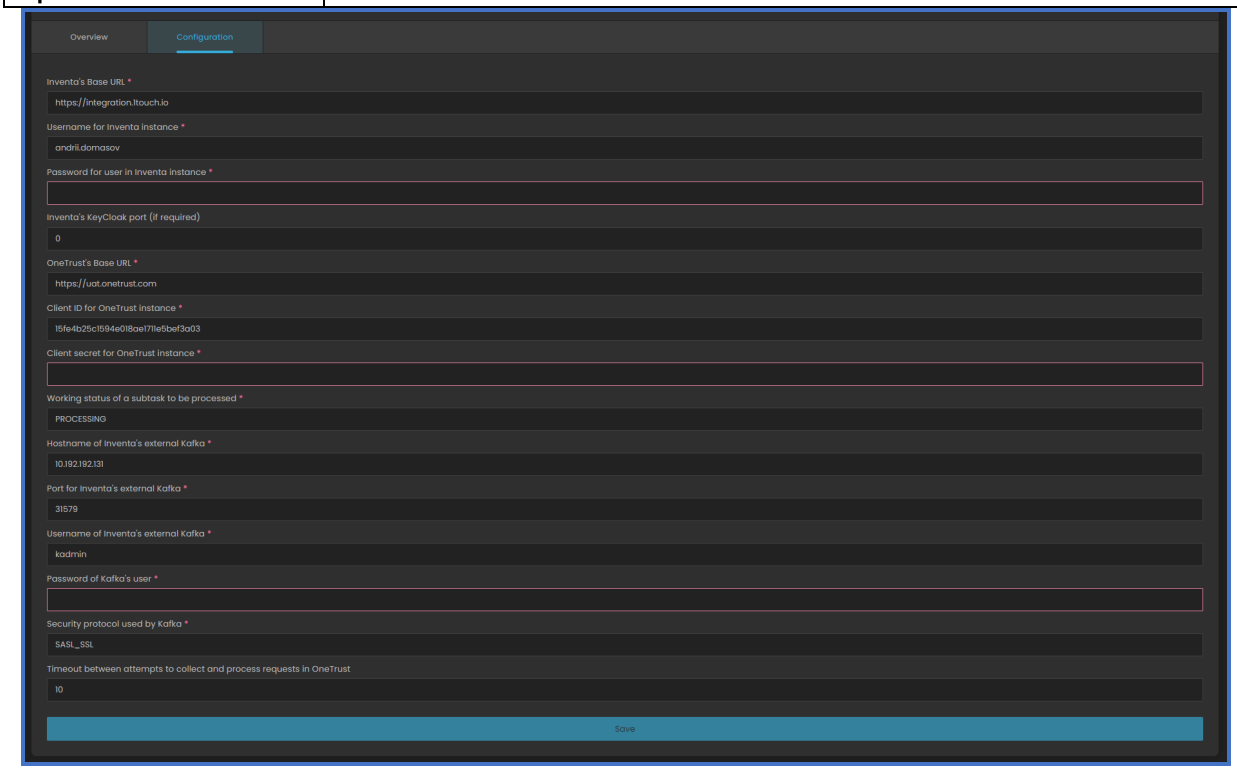


Figure 2: OneTrust configuration

SPLUNK CONFIGURATION

This integration allows you to monitor, analyze and configure reporting of IGDC activities and events via Splunk.

To configure the app settings, go to **Ecosystem > Syslog server extension for Splunk**. Then select the **Configuration** tab and configure the app settings.

Table 1: Splunk configuration

PARAMETER	DESCRIPTION
Report via HEC (See details in HTTP Event Collector examples)	
Splunk HEC Token	HEC token for connection to Splunk. *(Required)*
Event Host	Host shown in the event message. For example, IGDC. *(Required)*
Event Source	Source shown in the event message. For example, IGDC Kafka. *(Required)*
Event Source Type	Source type shown in the event message. For example, Kafka. *(Required)*
Report via file	
Message Storage	
Max records count in local .txt file	Maximal number of events that can be stored in the local file designated for reporting to Splunk.

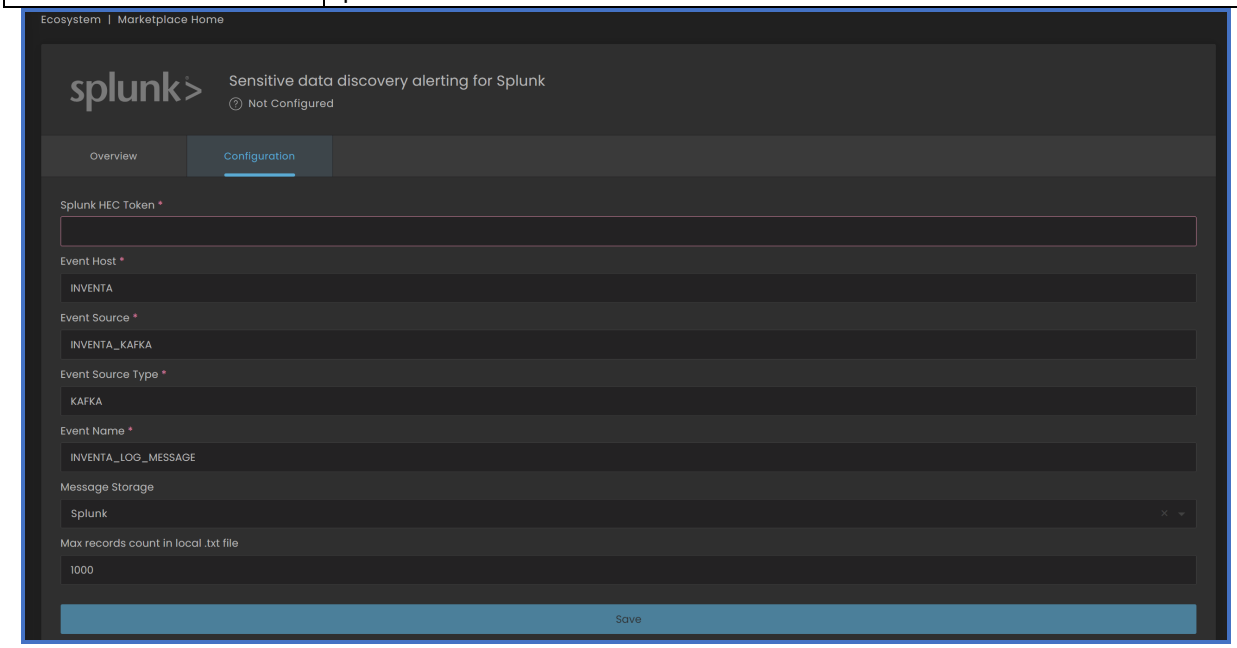


Figure 2: Splunk configuration

SERVICENOW CONFIGURATION

ServiceNow is an incident management solution that supports the ability to identify and log incidents, classify and prioritize incidents, assign incidents to appropriate users or groups, along with escalating, resolving, and reporting incidents.

IGDC discovers data sources, analyzes them, and classifies sensitive data in the data sources.

This integration app is triggered once IGDC discovers a preconfigured number of sensitive data locations (like tables in a database or files in a file share) in the data source. The app automatically creates an incident in ServiceNow for the data source and the appropriate number of sub-tasks for each sensitive data location. The sub-task will include the location path and the data elements discovered there.

To configure the app settings, go to **Ecosystem > Ticket creation in ServiceNow**. Then select the **Configuration** tab and configure the app settings.

Table 1: ServiceNow configuration

PARAMETER	DESCRIPTION
ServiceNow Host	Hostname of the SeviceNow. *(Required)*
ServiceNow user	Username of the integration app credentials in SeviceNow. *(Required)*
ServiceNow password	Password of the integration app credentials in SeviceNow. *(Required)*
Activate import data sources task	Toggle that activates/deactivates import of data sources from ServiceNow to the IGDC Data Source Catalog. Options: Yes, No.

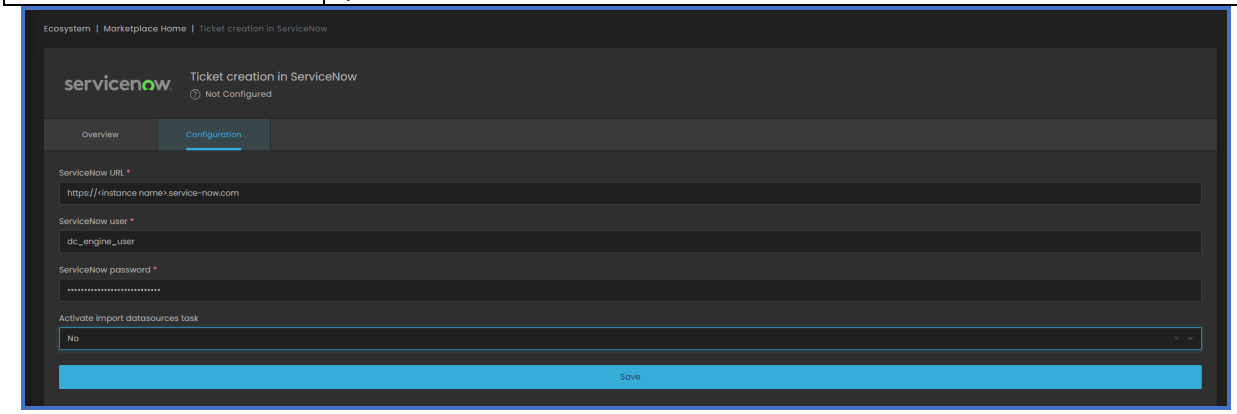


Figure 2: ServiceNow configuration

PORTAL26 SPECTRA CONFIGURATION

This integration enables the automatic encryption of files with sensitive data in Amazon S3 buckets, allowing users to manage their data more efficiently and ensure compliance with privacy regulations.

The Portal26 Spectra Java application can be configured to access and manage files in Amazon S3 buckets. IGDC analyzes the files in Amazon S3 buckets for personal or sensitive data existence.

This integration app uses Portal26 Spectra to automatically encrypt the files in Amazon S3 buckets, where IGDC found sensitive data. The integration app allows the user to automatically encrypt files containing personal data hosted in Amazon S3 buckets, tag/label files for encrypted objects in S3 buckets, send reports on workflow behavior, metrics of encrypted files, amount of pass/fail and reasons for failed results.

To configure the app settings, go to **Ecosystem > Portal26 Spectra**. Then select the **Configuration** tab and configure the app settings.

Table 1: Portal26 Spectra configuration

PARAMETER	DESCRIPTION
Portal26 Host	Hostname of the Portal26 Spectra. *(Required)*
Portal26 Port	Portal26 port for the integration app to connect to. *(Optional)*
Portal26 Scheme	Web scheme used by the target Portal26 platform. Options: https, http. *(Optional)*
AWS access_key_id	Access key of the integration app credentials in AWS. *(Required)*
AWS secret_access_key	Secret key of the integration app credentials in AWS. *(Required)*

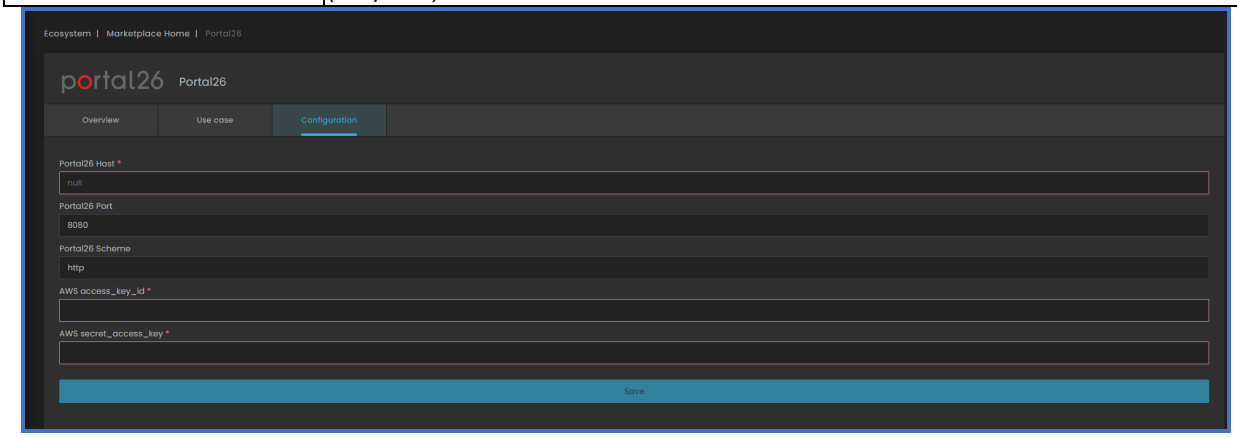


Figure 2: Portal26 Spectra configuration

POLICY MANAGEMENT

IGDC platform > Policy Engine assists in managing policies built for the IGDC integrations with other 3rd-party tools. Here you can:

- Review the configured policies in the **Policies** tab.
- Create, modify and remove policies via the policy wizard.

CONFIGURED POLICIES DASHBOARD

The **Policy Engine** page (IGDC Platform > Policy) represents the list of the configured policies with an ability to search, filter, sort, and manage them.

The policy engine dashboard shows the main information on the configured policies. To see the policy details, expand the desired policy entry.

Table 1: Policy properties

POLICY PROPERTY	DESCRIPTION
Collapsed view	
Policy name	Name of the policy, which is manually defined when adding/editing the policy in the policy wizard.
Action	Action triggered by the policy . The action is configured in the Target actions step of the policy wizard when adding/editing the policy.
Platform	Name of the 3rd party solution vendor, which IGDC is integrated with. You can filter by platform using the Vendor filter on the sidebar.
Hits	Score that reflects the frequency with which the policy was triggered by data matching the configured conditions. It is represented by two colors: green and red. **Green** shows the number of successfully triggered actions. **Red** shows the number of actions that failed to execute as expected.
Active	Current status of the policy. Options: active ( ), paused ( ).
Options icon ( )	Available actions: Pause, Activate, Edit, Delete. The **Pause** option deactivates the policy. This option is shown only for active policies. The **Activate** option activates the policy. This option is shown only for paused policies. The **Edit** option redirects you to the policy wizard. The **Delete** option initiates the removal of the policy.
Expanded view	
Policy description	Details of the policy defined in the policy wizard when adding/editing the policy.
Last modified	Date and time when the policy was last edited.
Condition	Condition that triggers the policy action (discovery of the defined data elements, data categories, data source type, URL). The conditions are configured in the policy wizard when adding/editing the policy.

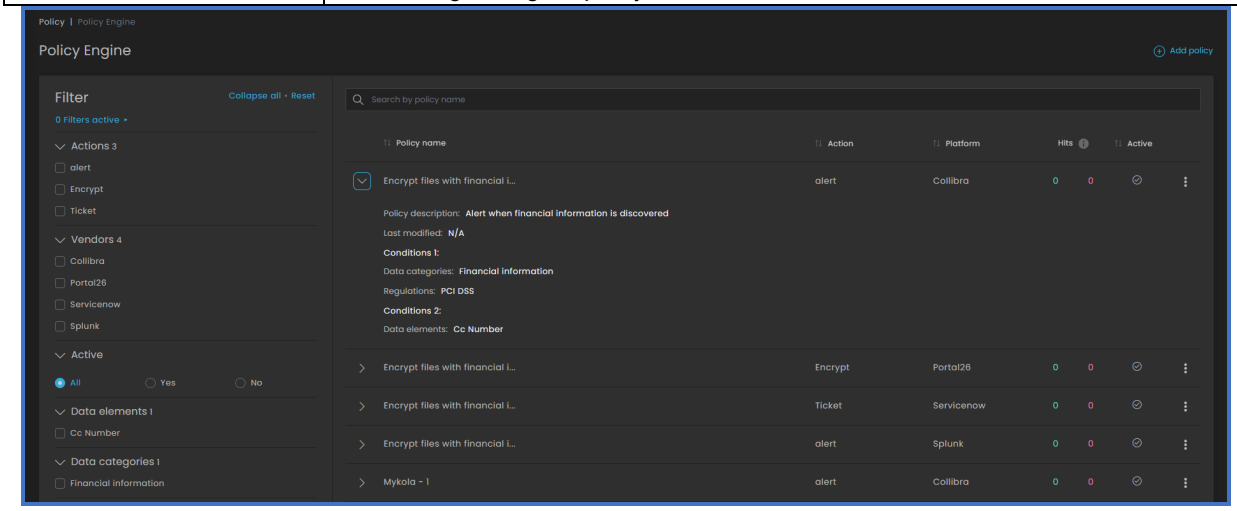


Figure 2: Policy Engine page

The Policy page offers the following options for sorting and ordering the policy entries: search bar, sidebar filters, order icons in the header.

Table 3: Dashboard entries sorting and ordering

SORTING/ORDERING	DESCRIPTION
Search bar (1)	Search for the desired policies by policy name using the search bar. Begin typing in the text box, and the dashboard will show only the entries with the text you entered.
Filters (2)	In the left sidebar, select the desired filters to see only the relevant entries. The options in the filters are dynamic, only the data present in the current policies is displayed as options. Filter options: action, vendors, active, data elements, data categories, data source types. **Action**: Show the policies triggered by the selected action. **Vendors**: Show the policies which include the integrations with the selected platform (vendor). **Active**: Show the policies with the selected status (yes - active, no - paused). **Data elements**: Show the policies where the selected data elements are configured as a triggering condition. **Data categories**: Show the policies where the selected data categories are configured as a triggering condition. **Data source types**: Show the policies where the selected data source types are configured as a triggering condition.
Order icons (3)	Click the order icon next to the desired parameter to order the policy entries. Options: Policy name (alphabetic), Action (alphabetic), Platform (alphabetic), Active-Paused.

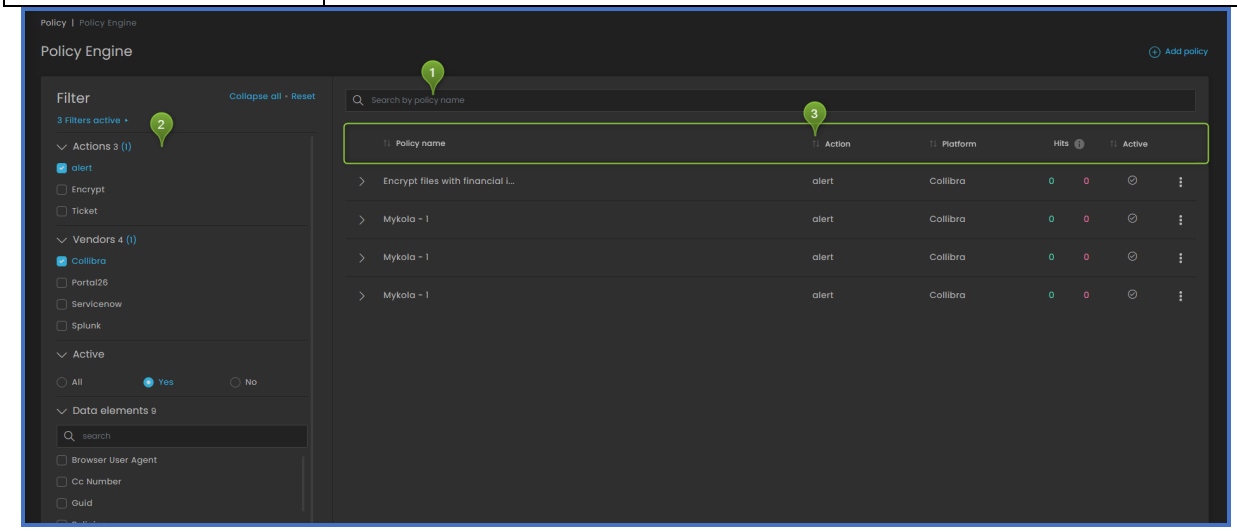


Figure 4: Sorting & ordering on the policy engine dashboard

CREATE POLICIES

1. On the **Policy Engine** page, click the **Add policy** button. The **Add policy** wizard will open.

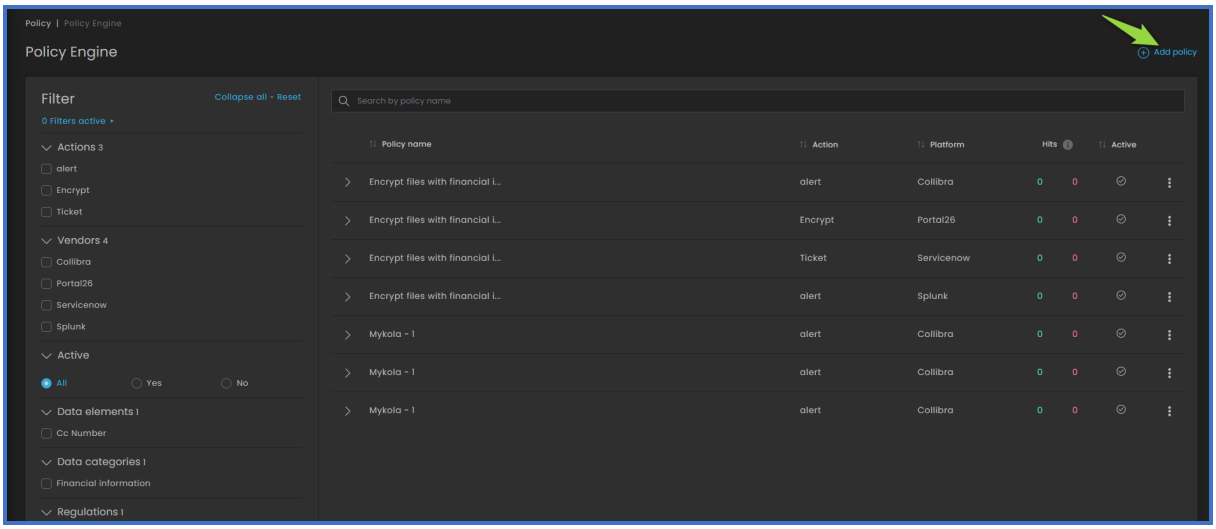
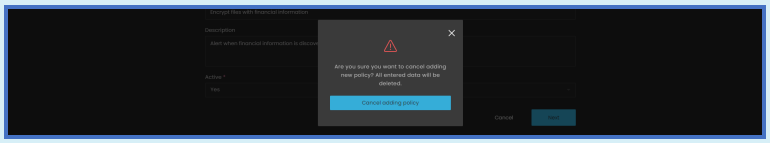


Figure 1: Add policy button on the Policy Engine page

You can stop the policy creation at any wizard step by clicking **X** in the upper right corner. Once you click **Cancel adding policy** in the confirmation popup, the wizard closes and all configurations are lost.



2. Fill the **Parameters** form and click **Next**.

Table 2: Parameters form

PARAMETER	DESCRIPTION
Policy name	Name of the policy shown on the **Policy Engine** page. You will be able to search by this name. *(Required)*
Description	Auxiliary information on the policy. It will be shown in the policy expanded view.
Active	Status of the policy upon creation. You can later change the status using the *Pause/Activate* buttons or in edit mode. Options: Yes, No. Select **Yes** to activate the policy upon creation. Select **No** to pause the policy upon creation.

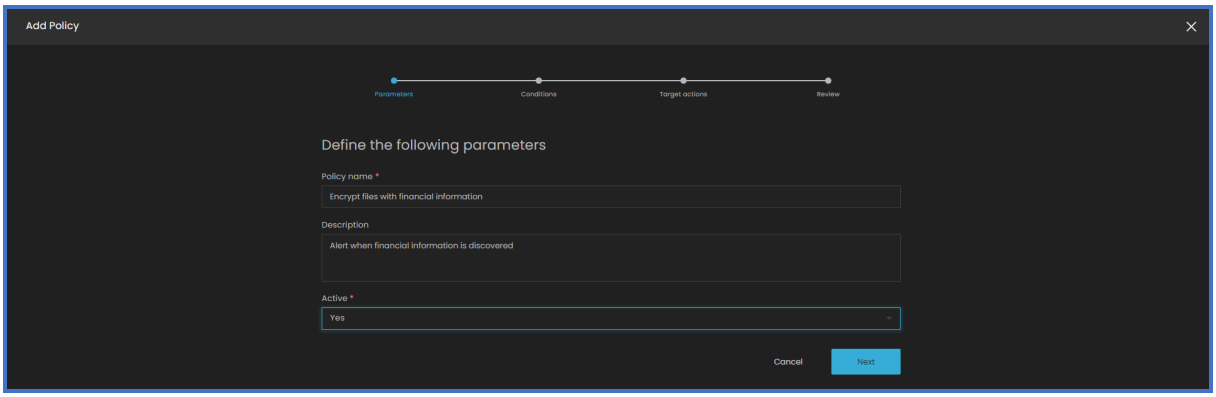


Figure 3: Parameters step of the policy wizard

3. Configure the conditions that will trigger the policy and click **Next**. The conditioning works as follows:

- At least one condition must be configured.
- You can configure multiple conditions by clicking **Add new condition** (**1**).
- You can delete all conditions except the first one by clicking **Delete the condition** (**2**).
- Within the condition, all parameters operate under AND rule, meaning all configured parameters must be met to trigger the policy.
- The conditions operate under OR rule, meaning the policy is triggered if all parameters are met within at least one condition.

Table 4: Condition parameters

PARAMETER	DESCRIPTION
Data elements	Select the data elements that will trigger the policy. Once IGDC discovers the specified data element(s) in a data source (e.g. credit card number, passport number, etc), the policy performs the relevant action. For example, once IGDC discovers a credit card number in a file, the policy performs the relevant action. You can find and configure the data elements in CM UI > Settings > Data recognition > Data element configuration.
Data category	Select the data categories that will trigger the policy. Once IGDC includes a data source in the specified data category(ies) (e.g. financial information, contact information, etc.), the policy performs the relevant action. You can find and configure the data categories in IGDC platform > Business context > Data categories.
Regulation	Select the regulations that will trigger the policy. Once IGDC tags a data source by the specified regulation(s) (e.g. PCI DSS, GDPR, etc.), the policy performs the relevant action. In IGDC, regulations are defined as part of a data category. You can assign regulations to data categories in IGDC platform > Business context > Data categories.
Data source type	Select the data source type that will trigger the policy. Once IGDC discovers a specified data source type (e.g. database, cloud storage, etc.) the policy performs the relevant action. You can find the data source types in CM UI > Inventory > Data Source Catalog.
Data source URL	Select the data source URL that will trigger the policy. Once IGDC discovers a data source with the specified URL, the policy performs the relevant action. You can find the data source types in CM UI > Inventory > Data Source Catalog.

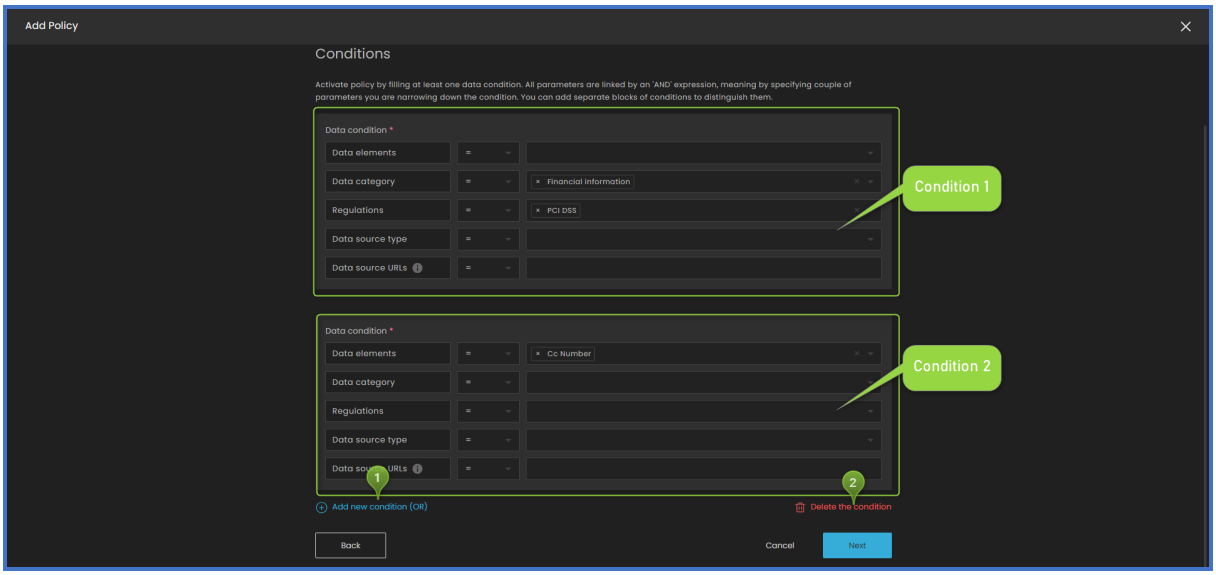


Figure 5: Conditions step of the policy wizard

4. Configure the action triggered by the policy, when the condition from the previous step is met.

To add a target action, select the 3rd-party vendor/platform from the **Solution** dropdown. Then select the desired action from the **Action** dropdown. Some solution+action pairs require auxiliary settings. Then you will see the auxiliary fields under the configured pair. For example, the Google+Label (target action 1 on screen) has no auxiliary properties; the Splunk+Alert pair (target action 2 on screen) has 1 auxiliary property - follow-up message syntax.

The actions work as follows:

- At least one target action must be configured.
- You can configure multiple target actions by clicking **Add new target action** (**1**).
- You can delete all target actions except the first one by clicking **Delete the target action** (**2**).
- All the target actions operate under AND rule, meaning the policy will trigger all the configured actions once the condition from the previous step is met.

Once all desired actions are configured, click **Next**.

Table 6: Target action properties

SOLUTION + ACTION	DESCRIPTION	
Collibra+alert	Create a new asset in Collibra and enrich it with data from IGDC. This helps you to ensure the sensitive data is monitored and is in compliance with appropriate policies and regulations.	
Google+label	Assign labels to the files on the Google drive to manage data more efficiently and ensure compliance with privacy regulations.	
OneTrust+ticket	Create a DSAR request in OneTrust and use IGDC info to populate it with enriched data.	
Portal26+encrypt	Trigger file encryption by Portal26 Spectra in Amazon S3 buckets.	
Alation+alert	Create a new asset in Alation and enrich it with data from IGDC. This ensures the Alation's data governance capabilities cover all you data assets.	
Splunk+alert	Send a syslog-like message to Splunk. The message contains metadata like timestamp of discovery, discovered data element, full data source location, etc.	
	Property	**Description**

SOLUTION + ACTION	DESCRIPTION	
	Follow-up message syntax *(Optional)*	Define the alert message syntax based on Jinja templates that control the content of the alert you send to the integrated solution. The field accepts any strings and several variables that will be populated for a specific alert message. Accepted variables: url; path; owner; entities; found_time; pii_ts. url: URL of the data source where personal data has been discovered. For example, jdbc:oracle:thin:@192.168.1.1:11521:XE (database), smb://192.168.1.1/path/to/dir(file share), etc. path: Direct path to the data source where personal data has been discovered. Database path format: db.schema.table, e.g. db1.schema1.table2. File shares format: /path/to/file.extension. owner: Owner of resource. Applied to files only. entities: List of data elements discovered in the data source. For example, CC_NUMBER PASSPORT_NUMBER EMAIL_ ADDRESS. List separator: space symbol ( ) . found_time: Timestamp when the data source location message was discovered by the integration app. pii_ts: Timestamp when IGDC discovered the data source. The text field expects variables to be enclosed in double braces with variable names inside like {{url}}. For example: Syntax input: {{entities}} entities discovered in {{path}} location of data source: {{url}} at {{pii_ts}} Result: CC_TYPE NATIONAL_ID entities discovered in xls\1000\XLS-1000-(527).
ServiceNow+ticket	Automatically create an incident in ServiceNow and the appropriate number of sub-tasks for each sensitive data location. The sub-task will include the location path and the data elements discovered there.	
	Property	**Description**
	Events counter *(Required)*	Number of sensitive data locations required for the subtask creation in the ticket. For example, if the counter is set to 100, and IGDC discovers 500 files in an S3 bucket with the configured data elements, the integration app will create a ticket for the S3 bucket in Service now and 5 subtasks (1 subtask for every 100 files with sensitive data elements).
	Assignment Group ID *(Optional)*	ID of the ServiceNow user group the tickets will be assigned to.
	Assignment User ID *(Optional)*	ID of the ServiceNow user the tickets will be assigned to.

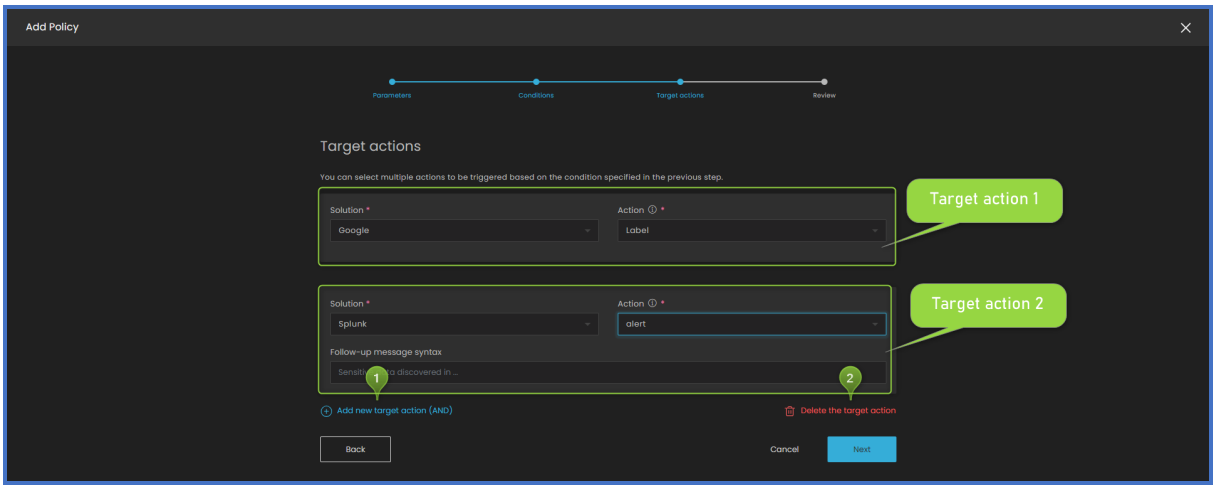


Figure 7: Target actions step of the policy wizard

5. Review the summary of the policy configuration on all previous steps. If you wish to make any changes, click the (**Edit**) icon for the desired section, and you will be redirected to the relevant step of the policy wizard. You can also click **Back** to return to the previous step or click **Cancel** to close the policy wizard.

If the policy configuration is correct, click the **Add Policy** button. Once you click **Add Policy**, the policy wizard closes, the new policy is added at the bottom of the Policy Engine Dashboard, and the corresponding notification is shown in the lower right corner 

.

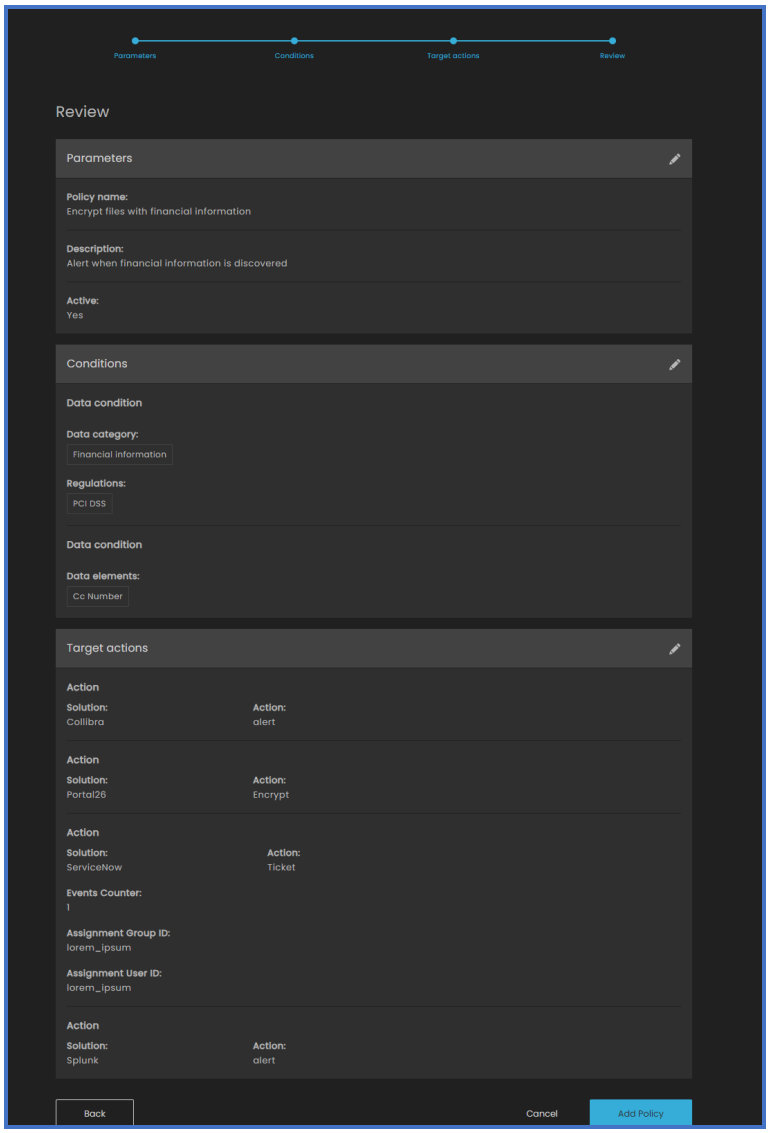
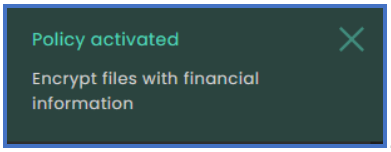


Figure 8: Review step of the policy wizard

ACTIVATE & PAUSE POLICIES

You can activate & pause policies on the Policy Engine dashboard (IGDC Platform > Policy) or in policy edit mode.

1. To activate a policy, click the (**Options**) icon (**1**) for the desired policy and select the **Activate** option (**2**). Once you click **Activate**, the policy status changes to active ( ), and the corresponding notification appears in the lower right corner: 

.

The **Activate** option is available only for policies with *paused* status.

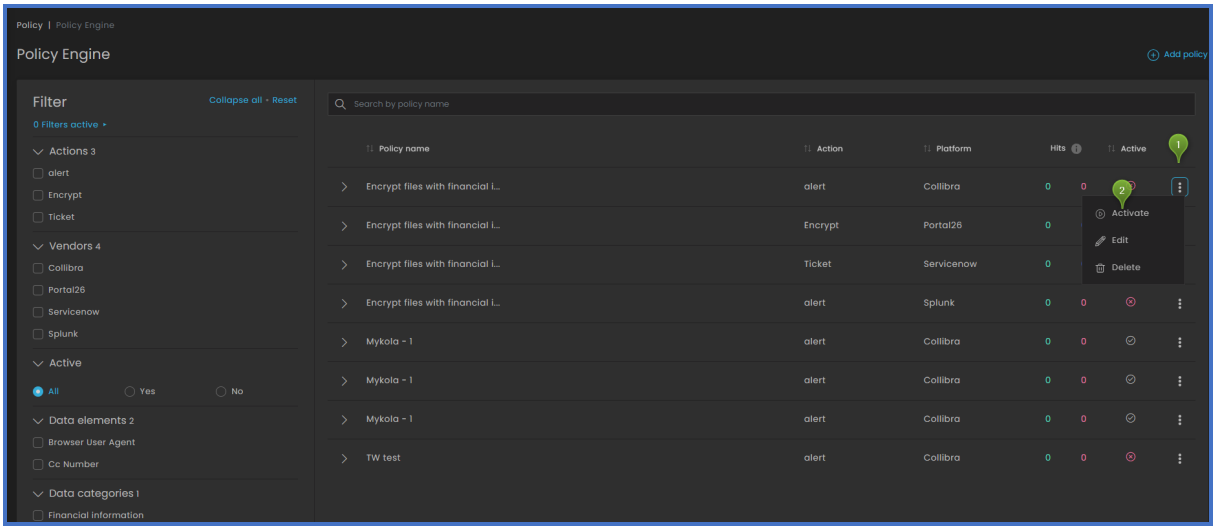
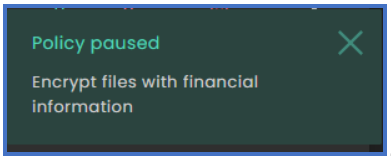


Figure 1: Activating a policy

2. To pause a policy, click the (**Options**) icon (**1**) for the desired policy and select the **Pause** option (**2**). Once you click **Pause**, the policy status changes to paused ( ), and the corresponding notification appears in the lower right corner: 

.

The **Pause** option is available only for policies with *active* status.

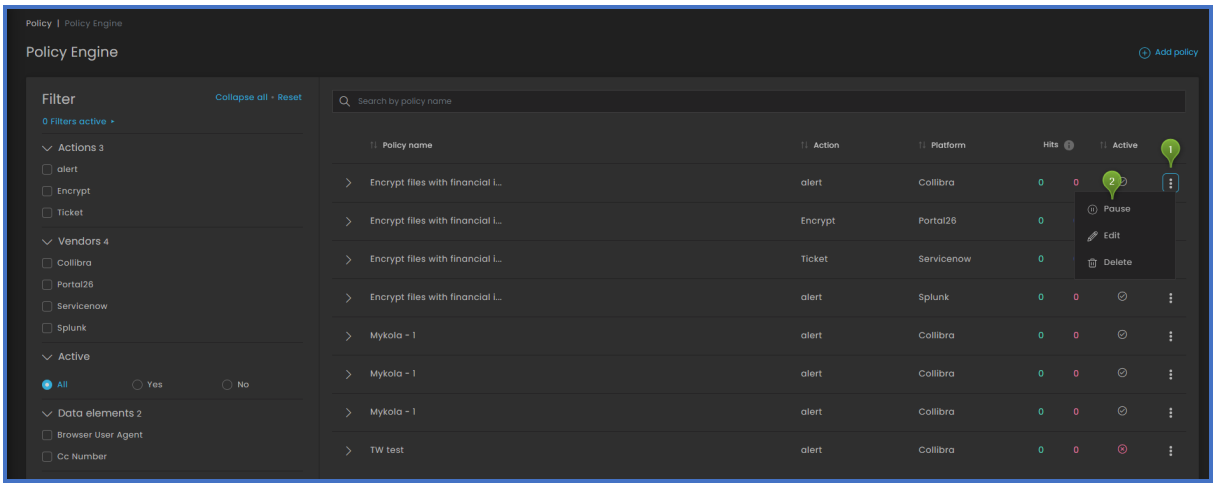


Figure 2: Pausing a policy

EDIT AND DELETE POLICIES

The Policy Engine page (IGDC Platform -> Policy) allows you to edit and delete the existing policies.

1. To edit a policy, click the click the ⋮ (**Options**) icon for the desired policy and select the **Edit** option. IGDC will redirect you to the policy editing wizard (same as the policy adding wizard).

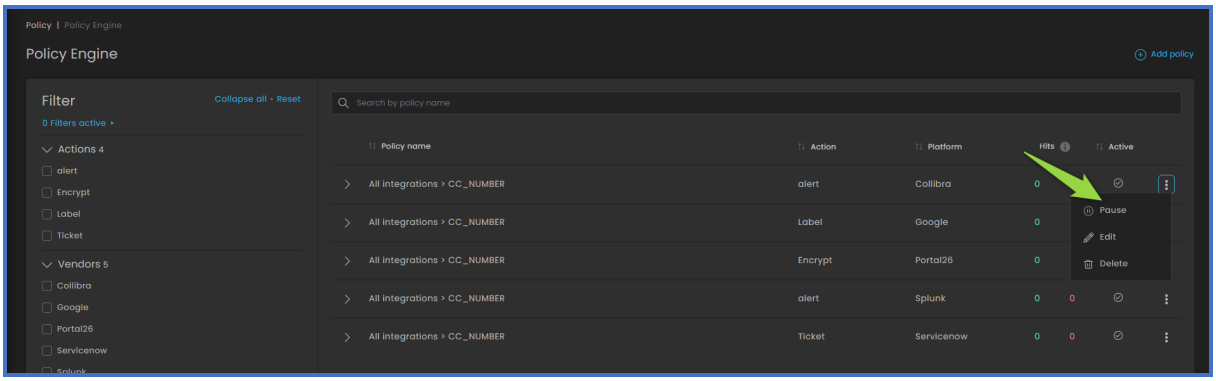


Figure 1: Policy editing

2. To delete a policy, click the ⋮ (**Options**) icon for the policy you wish to remove and select the **Delete** option.

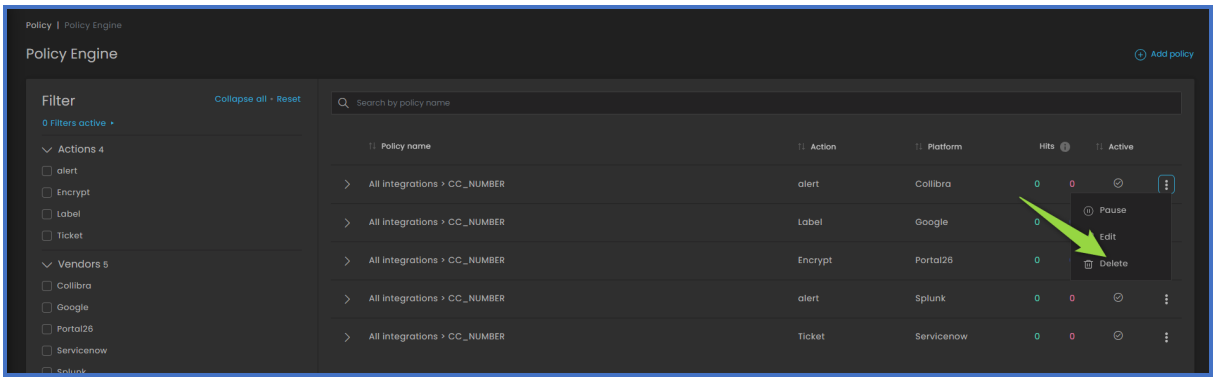


Figure 2: Policy deletion

In the deletion confirmation window, click **Delete policy** to confirm the deletion. To exit without removing the policy, click **X** in the upper right corner of the popup.

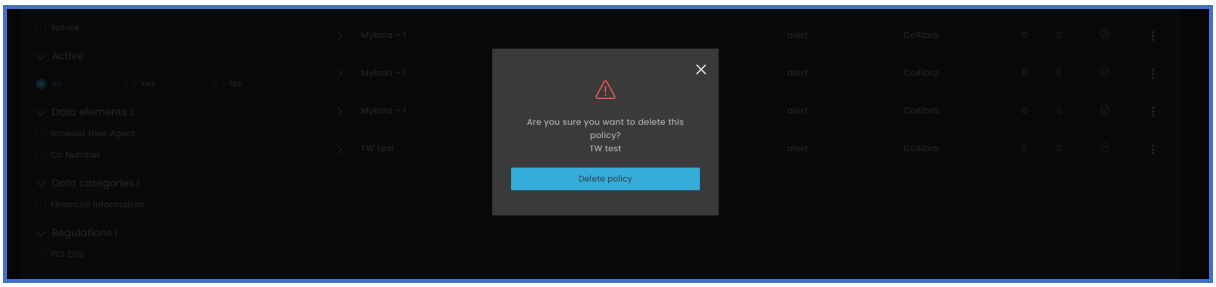
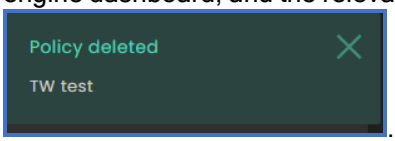


Figure 3: Policy deletion confirmation popup

Once you click **Delete** policy, the confirmation popup closes, the subject policy is removed from the policy engine dashboard, and the relevant notification is shown in the lower right corner:



.